CLAIMS

We claim:

1. A method for modifying entries in an Identity System, comprising the steps of:

creating a first entry for said Identity System, said first entry includes a first set of attributes based on a first set of one or more classes; and

removing a subset of said first set of attributes from said entry after said step of creating said first entry.

2. A method according to claim 1, wherein:

said first set of one or more classes includes a structural class and a first set of one or more auxiliary classes.

3. A method according to claim 1, wherein:

said step of removing includes a step of removing one or more auxiliary classes from said entry, said one or more auxiliary classes are associated with said subset of said first set of attributes.

4. A method according to claim 3, wherein said step of removing one or more auxiliary classes from said entry includes the steps of:

removing a first auxiliary class associated with said subset of said first set of attributes; and

removing auxiliary classes that are superior to said first auxiliary class and that are not superior to any auxiliary classes that remain part of said entry.

5. A method according to claim 3, wherein:

said subset of said first set of attributes includes data stored in said attributes; and

said step of removing a subset of said first set of attributes includes removing said data.

6. A method according to claim 1, wherein said step of removing a subset of said first set of attributes includes the steps of:

identifying a set of auxiliary classes in a user interface;

receiving a selection of one or more of said auxiliary classes via said user interface; and

removing said selected one or more of said auxiliary classes.

7. A method according to claim 1, wherein said step of removing a subset of said first set of attributes includes the steps of:

identifying a set of attributes in a user interface;

receiving a selection of said subset of said first set of attributes via said user interface; and

removing said subset of said first set of attributes from said entry.

8. A method according to claim 1, further comprising the step of:

adding new attributes to said entry after said step of creating.

9. A method according to claim 8, wherein:

said step of adding new attributes includes adding one or more auxiliary classes associated with said new attributes to said entry.

10. A method according to claim 8, wherein said step of adding new attributes includes the steps of:

adding one or more auxiliary classes associated with said new attributes to said entry; and

adding classes to said entry that are not already part of said entry and are superior to said one or more auxiliary classes associated with said new attributes.

11. A method according to claim 8, wherein said step of adding new attributes includes the steps of:

identifying a set of auxiliary classes in a user interface;

receiving a selection of one or more of said auxiliary classes via said user

interface; and

adding said selected one or more of said auxiliary classes.

12. A method according to claim 8, wherein said step of removing a subset of said first set of attributes includes the steps of:

identifying a set of attributes in a user interface;

receiving a selection of said new attributes via said user interface; and

adding one or more auxiliary classes associated with said new attributes to said entry.

13. A method according to claim 8, wherein:

said steps of creating, adding and removing are performed by an integrated identity and access system; and

said an integrated identity and access system is capable of evaluating said new attributes to authorize a user to access a resource.

14. A method according to claim 8, wherein:

said entry is a group entry; and

at least one of said new attributes stores a rule defining dynamic membership for said group entry.

15. A method according to claim 8, wherein:

said entry is a group entry; and

at least one of said new attributes stores a subscription policy for said group entry.

16. A method according to claim 1, wherein:

said steps of creating and removing are performed by an integrated identity and access system.

17. A method according to claim 1, wherein:

said entry is a group object; and

said step of creating includes instantiating said group object.

18. A method according to claim 17, wherein:

said step of removing includes a step of removing one or more auxiliary classes from said group object, said one or more auxiliary classes are associated with said subset of said first set of attributes.

19. A method according to claim 18 wherein said step of removing one or more auxiliary classes from said group object includes the steps of:

removing a first auxiliary class associated with said subset of said first set of attributes; and

removing classes that are superior to said first auxiliary class and that are not superior to any auxiliary classes that remain part of said entry.

20. A method according to claim 17, further comprising the step of:

adding new attributes to said entry after said step of creating, said step of adding new attributes includes adding one or more auxiliary classes associated with said new attributes to said entry.

21. A method according to claim 17, wherein:

said group object is stored in an LDAP directory.

22. One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

creating a first entry for said Identity System, said first entry includes a first set of attributes based on a first set of one or more classes; and

removing a subset of said first set of attributes from said entry after said step of creating said first entry.

23. One or more processor readable storage devices according to claim 22,

wherein:

said step of removing includes a step of removing one or more auxiliary classes from said entry, said one or more auxiliary classes are associated with said subset of said first set of attributes.

24. One or more processor readable storage devices according to claim 23, wherein said step of removing one or more auxiliary classes from said entry includes the steps of:

removing a first auxiliary class associated with said subset of said first set of attributes; and

removing classes that are superior to said first auxiliary class and that are not superior to any auxiliary classes that remain part of said entry.

25. One or more processor readable storage devices according to claim 22, wherein said method further comprises the step of:

adding new attributes to said entry after said step of creating, said step of adding new attributes includes adding one or more auxiliary classes associated with said new attributes to said entry.

26. One or more processor readable storage devices according to claim 25, wherein said step of adding new attributes includes the steps of:

adding one or more auxiliary classes associated with said new attributes to said entry; and

adding classes to said entry that are not already part of said entry and are superior to said one or more auxiliary classes associated with said new attributes.

27. One or more processor readable storage devices according to claim 22, wherein:

said steps of creating and removing are performed by an integrated identity and access system.

28. One or more processor readable storage devices according to claim 22,

wherein:

said entry is a group object; and

said step of creating includes instantiating said group object.

29. One or more processor readable storage devices according to claim 28, wherein:

said step of removing includes a step of removing one or more auxiliary classes from said group object, said one or more auxiliary classes are associated with said subset of said first set of attributes.

30. One or more processor readable storage devices according to claim 29, wherein said step of removing one or more auxiliary classes from said group object includes the steps of:

removing a first auxiliary class associated with said subset of said first set of attributes; and

removing classes that are superior to said first auxiliary class and that are not superior to any auxiliary classes that remain part of said entry.

31. One or more processor readable storage devices according to claim 28, wherein said method further comprises the step of:

adding new attributes to said entry after said step of creating, said step of adding new attributes includes adding one or more auxiliary classes associated with said new attributes to said entry.

32. One or more processor readable storage devices according to claim 28, wherein:

said group object is stored in an LDAP directory.

33. An apparatus that can be used to manage Identity System entries, comprising:

a communication interface; and

one or more processors in communication with said communication interface, said one or more processors perform a method comprising the steps of:

creating a first entry for said Identity System, said first entry includes a first set of attributes based on a first set of one or more classes, and

removing a subset of said first set of attributes from said entry after said step of creating said first entry.

34. An apparatus according to claim 33, wherein:

said step of removing includes a step of removing one or more auxiliary classes from said entry, said one or more auxiliary classes are associated with said subset of said first set of attributes.

35. An apparatus according to claim 34, wherein said step of removing one or more auxiliary classes from said entry includes the steps of:

removing a first auxiliary class associated with said subset of said first set of attributes; and

removing auxiliary classes that are superior to said first auxiliary class and that are not superior to any auxiliary classes that remain part of said entry.

36. An apparatus according to claim 33, wherein said method further comprises the step of:

adding new attributes to said entry after said step of creating, said step of adding new attributes includes adding one or more auxiliary classes associated with said new attributes to said entry.

37. An apparatus according to claim 36, wherein said step of adding new attributes includes the steps of:

adding one or more auxiliary classes associated with said new attributes to said entry; and

adding auxiliary classes to said entry that are not already part of said entry and are superior to said one or more auxiliary classes associated with said new attributes.

38. An apparatus according to claim 33, wherein:

said steps of creating and removing are performed by an integrated identity and access system.

39. An apparatus according to claim 33, wherein:

said entry is a group object; and

said step of creating includes instantiating said group object.

40. An apparatus according to claim 39, wherein:

said step of removing includes a step of removing one or more auxiliary classes from said group object, said one or more auxiliary classes are associated with said subset of said first set of attributes.

41. An apparatus according to claim 40 wherein said step of removing one or more auxiliary classes from said group object includes the steps of:

removing a first auxiliary class associated with said subset of said first set of attributes; and

removing auxiliary classes that are superior to said first auxiliary class and that are not superior to any auxiliary classes that remain part of said entry.

42. An apparatus according to claim 39, wherein said method further comprises the step of:

adding new attributes to said entry after said step of creating, said step of adding new attributes includes adding one or more auxiliary classes associated with said new attributes to said entry.

43. An apparatus according to claim 39, wherein said group object is stored in an LDAP directory.